Notice of Allowability	Application No.	Applicant(s)	
	09/916,557	DUVAL, DONALD E.	
	Examiner	Art Unit	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *RCE filed 02/07/2007*.

2. ☒ The allowed claim(s) is/are *11,13-29,32 and 33*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *held on 02/27/2007* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

1. The request filed February 07, 2007 for a request for continued examination (RCE) under 37 CFR 1.114 based on patent application 09/916,557 is acceptable and an RCE has been established.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with **Lori A. Gordon** Reg. No 50,633 on 02/27/2007.

The application has been amended as follows: In the claims

3. (canceled)

~~3~~ 32. (currently amended) An accelerator ~~A system~~ as recited in claim 11 ~~30~~, further comprising:

a storage unit coupled to the encryption accelerator arranged to store at least a portion of the data to be encrypted.

10. (canceled)

~~10~~ 33. (currently amended) An accelerator ~~A system~~ as recited in claim 11 ~~30~~, wherein the encryption accelerator is selectively operable in an Initial Mode and a Continuation

mode wherein the Initial Mode the accelerator ~~system~~ operates in a sequential manner whereas in the continuation mode the state memory is reloaded with stored state memory values.

11. (currently amended) An encryption accelerator arranged to encrypt and decrypt data formed of a plurality of bytes using an RC4 stream cipher, comprising:
a combinational logic block arranged to perform a pre-determined logic operation on selected input values;
a state memory array coupled to the combinational logic block having a plurality of memory locations wherein the state memory is configured to store a plurality of substitution values associated with the RC4 stream cipher, each substitution value stored in a separate memory location; and
a state machine coupled to the combinational logic block and the state memory, the state machine configured to:

initialize via hardware an incrementing pattern of substitution values in the state memory, each substitution value stored in a separate memory location,

~~perform~~ direct a first RC4 shuffling operation using a portion of a key array received from a system memory via an interface external to the encryption accelerator, by which the plurality of substitution values are moved to different memory locations within the state memory, wherein the first RC4 shuffling operation is performed concurrently with the receipt of the portion of the key array, wherein the first RC4 shuffling operation is completely performed within the encryption accelerator,

generate a random byte as a result of a second RC4 shuffling operation;

byte-wise transfer a portion of the data to the combinational logic block as a first input value,

transfer the generated random byte to the combinational logic as a second input value,

logically operate on the first and second input values by the combinational logic to form a resulting data byte, and outputting the resulting data byte , wherein the encryption accelerator uses substantially no central processing unit resources to perform the RC4 stream cipher.

23. (currently amended) The ~~system~~ accelerator of claim 11 ~~30~~, wherein the state machine is further configured to direct a second RC4 shuffling to generate a random byte.

24. (currently amended) The ~~system~~ accelerator of claim 23, wherein the hardware-based encryption accelerator includes a combinational logic block configured to exclusive OR the generated random byte with a byte of the data.

25. (currently amended) A method for performing an RC4 stream cipher in a hardware-based cryptographic accelerator including a state memory having a plurality of memory locations, wherein the state memory is configured to store a plurality of substitution values associated with the RC4 stream cipher, each substitution value stored in a separate memory location and a state machine coupled to the state memory, the method comprising:

(a) initializing ~~a~~ the memory locations of the state memory ~~having a plurality of memory locations~~ with an incrementing pattern of substitution values;

(b) receiving, at the hardware-based encryption accelerator via an interface external to the cryptographic accelerator, a portion of a key array;

(c) upon direction of [[a]] the state machine, shuffling the pattern of substitution values in the state memory using an RC4 shuffling operation by which the plurality of substitution values are moved to different memory locations within the state

memory, wherein the shuffling is performed concurrently with the receipt of the portion of the key array , and wherein the shuffling operation is completely performed within the cryptographic accelerator; and

(d) repeating steps (b) and (c) until each portion of the key array has been received ,

wherein the cryptographic accelerator uses substantially no central processing unit resources to perform the RC4 stream cipher.

30-31. (canceled)

Allowable Subject Matter

2. **Claims 1-2, 4-9 and 12** were previously canceled.

As the result of Examiner's amendment,

- **Claim 3** is amended and is replaced by claim 32 likewise **claim 10** is amended and replaced by claim 33. Thus, **claims 3 and 10 are canceled**.
- **Claims 30-31** are also canceled.
- **Claims 11, 23-25** have also been amended.

Thus **claims 1-10, 12 and 30-31 are canceled** and **claims 11, 13-29 and 32-33** remain in the application.

3. **Claims 11, 13-29 and 32-33** are allowed.

4. The following is an examiner's statement of reasons for allowance:

5. Referring to **the independent claims 11 and 25** the art on the record, the combination of the references, namely **Vano and Schneier** discloses all the limitation of the claims before it is amended as shown below.

Referring to the independent claims 11 and 25 Vano discloses

- **An encryption accelerator** *[Figure 1, ref. Num "550"] (An encryption accelerator met to be "Cryptographic co-processor" shown on figure 1, ref. Num "550")* **comprising:**

- **A combinational logic block arranged to perform a pre-determined logic operation on selected input values;***[Figure 1, ref. Num "576" and column 6, lines 50-55) ("As explained on column 6, lines 50-55 a Permuter shown on figure 1, ref. Num "576" performs cryptographic operations as explained on column 6, lines 50-55)*

- **A state memory array***[Figure 1, ref. Num "554" or "State Register"]* **arranged to store a plurality of state memory values;***[Column 6, lines 19-22;](state memory values is met "channel program states")*

- **A state machine coupled to the state memory array configured to perform of encryption algorithm.***[Figure 1, ref. Num "558", "control register"; column 6, lines 31-36]*

- **Performing a shuffling operations using a portion of the key array, wherein the shuffling operation is performed concurrently with the receipt of a portion of the key array,***[Column 6, lines 54-59; Column 6, lines 19-21; column 8, lines 20-24](Permuters select bits from state register as explained on column 6, lines 54-59 and the state register contains channel*

program as explained on column 6, lines 19-21 and the key is also contained in the channel program as explained on column 8, lines 20-24)

- **Byte-wise transferring the data to the combinational logic block as a first input value, and transferring a corresponding state memory value to the combinational logic as a second input value; logically operate on the first and the second input values by the combinational logic to form a resulting/an encrypted data byte;***[figure 1](As shown on figure 1, it is implicit to transfer data from the data register "564" and the state register "554" to the permuter which is shown on figure 1, ref. Num "576")* and

- **Outputting the resulting/encrypted data byte.**[Figure 1, ref. Num "566", "data out register"]

Vano does not explicitly disclose

- **Initializing via hardware of an incrementing pattern in the state memory array without loading the incrementing pattern from an external memory**

- **Wherein the shuffling operation is the RC4 shuffling operation,**

- **Byte-wise transferring of data**

However, in the same field of endeavor, **Schneier** discloses

- Storing of an incrementing pattern in the state memory array with/without loading the incrementing pattern from an external memory *[Page 397, lines 23] (filling the s-box linearly)*

- Wherein the RC4 shuffling operation includes moving each of the plurality of state memory values based upon the secret key.*[Page 397, lines 23-page 398 line 3]*

- Byte-wise transferring of data *[Page 397, lines 21-23](S-box-entries are exclusively OR'd byte-wise with plaintext)*

- However, the combination of **Vano and Schneier**, does not explicitly disclose some of the functional limitations which are incorporated to the **respective independent claims 11 and 25** by the examiner's amendment.

The combination of **Vano and Schneier** does not discloses, the following functional limitation recited in claims 11 and 25, "direct a first RC4 shuffling operation using a portion of a key array received from a system memory via an interface external to the encryption accelerator, by which the plurality of substitution values are moved to different memory locations within the state memory, wherein the first RC4 shuffling operation is performed concurrently with the receipt of the portion of the key array"

And the following limitation recited in claims 11 and 25

"wherein the encryption accelerator uses substantially no central processing unit resources to perform the RC4 stream cipher.

In vano reference the key is not received via an interface external to the encryption accelerator, the key is inside the encryption acceleration/cryptographic co processor shown on figure 1, ref. Num "558".

In particular the key is located inside the state register within the encryption accelerator/cryptographic co processor. The state register contains channel program as explained on column 6, lines 19-21 and the key is also contained in the channel program as explained on column 8, lines 20-24

Furthermore, Neither Vano nor Schneier teaches that the encryption accelerator uses substantially no central processing unit resources to perform the RC4 stream cipher. Actually this is the drawback of the RC4 algorithm.

- None of the prior art of record taken singularly of in combination teaches or suggests such a method/an accelerator with the functional limitation added to the respective independent claims 11 and 25 together with all the limitations previously recited in respective independent claims **11 and 25.**

For the reasons provided above, the amended independent claims **11 and 25** are allowed.

6. **The dependent claims 13, 14-24, 26-29 and 32-33 which are dependent on the respective independent claims 11 and 25** being further limiting to the independent claims, definite and enabled by the specification are also allowed. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submission should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am --4: 30 pm). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA
S.L.
02/28/2007

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100